(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
30 juin 2005 (30.06.2005)

PCT

(10) Numéro de publication internationale
WO 2005/060205 A1

(51) Classification internationale des brevets[7] :
H04L 29/06, G06F 17/30

(21) Numéro de la demande internationale :
PCT/FR2004/003252

(22) Date de dépôt international :
16 décembre 2004 (16.12.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0314833 17 décembre 2003 (17.12.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **MORIN, Benjamin** [FR/FR]; 22, rue des Croisières, F-14000 Caen (FR). **DEBAR, Hervé** [FR/FR]; 7, rue des Semailles, F-14111 Louvigny (FR).

(74) Mandataires : **JOLY, Jean-Jacques** etc.; Cabinet Beau de Loménie, 158, rue de l'Université, F-75340 Paris Cedex 07 (FR).

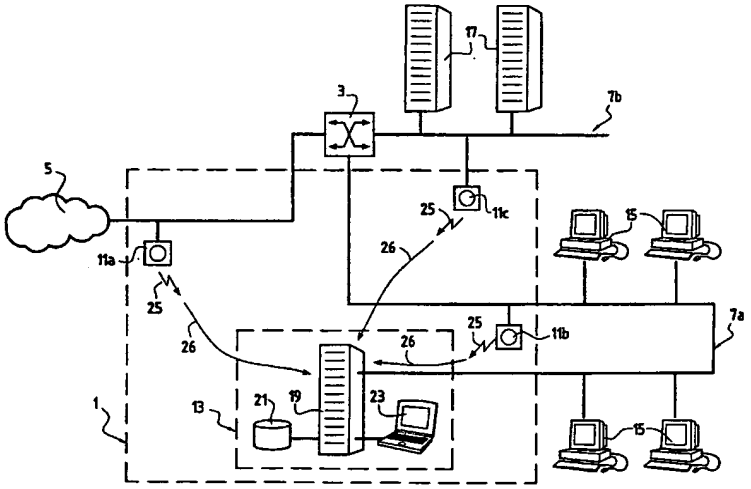
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH,

[Suite sur la page suivante]

(54) Title: METHOD FOR MANAGING A SET OF ALARMS EMITTED BY SENSORS FOR DETECTING INTRUSIONS OF A INFORMATION SECURITY SYSTEM

(54) Titre : PROCEDE DE GESTION D'UN ENSEMBLE D'ALERTES ISSUES DE SONDES DE DETECTION D'INTRUSIONS D'UN SYSTEME DE SECURITE D'INFORMATIONS.



(57) Abstract: The invention relates to a method for managing a set of alarms emitted by intrusion detecting sensors (11a, 11b, 11c) of an information security system (1) comprising an alarm managing system (13), wherein each alarm is identified by an alarm identifier and an alarm content consisting in assigning a description comprising a conjunction of a plurality of valued attributes allocated to a plurality of attribute ranges to each alarm emitted by said intrusion detecting sensors (11a, 11b, 11c), organising the valued attributes allocated to each attribute range into a taxonomic structure defining generalisation ratios between said valued attributes and the plurality of attribute ranges forming the structure of taxonomic structures, completing the description of each said alarm by a set of values induced by the taxonomic structures from the valued attribute of said alarms in order to form completed alarms and in storing said completed alarms in a logic files (21) in such a way that it is possible to reference thereon.

[Suite sur la page suivante]

WO 2005/060205 A1

GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de gestion d'un ensemble d'alertes issues de sondes de détection d'intrusions (11a, 11b, 11c) d'un système de sécurité d'informations (1) comportant un système de gestion d'alertes (13), chaque alerte étant définie par un identifiant d'alerte et un contenu d'alerte, le procédé comportant les étapes suivantes -associer à chacune des alertes issues des sondes de détection d'intrusions (11a, 11b, 11c), une description comportant une conjonction d'une pluralité d'attributs valués appartenant à une pluralité de domaines d'attributs ; -organiser les attributs valués appartenant à chaque domaine d'attributs en une structure taxinomique définissant des relations de généralisation entre lesdits attributs valués, la pluralité des domaines d'attributs formant ainsi une pluralité de structures taxinomiques ; -compléter la description de chacune desdites alertes par des ensembles de valeurs induites par les structures taxinomiques à partir des attributs valués desdites alertes pour former des alertes complètes ; -stocker lesdites alertes complètes dans un système de fichiers logique (21) pour en permettre la consultation.